



Consolidated Technology Services • WA

State Data Center

Firewall Migration Guide

Version 1.0
April 24, 2013

Prepared by:
Steve Lovaas, Enterprise Projects Client Liaison

Contents

DOCUMENT REVISION HISTORY	3
INTRODUCTION AND PURPOSE	4
DOCUMENT STRUCTURE	4
DOCUMENT SCOPE	5
SECTION 1 – MPLS CONNECTORS (SIMPLE SECURITY POLICY)	6
MIGRATION TASKS	6
APPENDIX A – MPLS CONNECTORS (SIMPLE SECURITY POLICY) MIGRATION CHECKLIST	10

Document Revision History

Description of Change	Page or Section	Date Revised	Reviser
Published first draft	All	4/24/13	Steve Lovaas

Introduction and Purpose

The purpose of this Migration Guide is to define the steps that Consolidated Technology Services (CTS) and customer staff will take to complete readiness tasks necessary for the migration of systems to the State Data Center (SDC). It also contains the migration and post migration tasks needed to fully complete the migration effort.

This Guide documents the key activities to be coordinated by the customer's Agency Implementation Coordinator (AIC) in preparation for each system migration. These activities are summarized in a checklist that will be used to track completed activities and when complete signifies that the system is ready for migration scheduling. Completion of these activities is critical to migration success and will help to minimize any unplanned service disruption. The AIC serves as the primary customer contact and is responsible for coordinating the internal customer activities stated in the Guide.

When all tasks are complete the AIC will submit customer acceptance for cutover to the CTS Enterprise Projects Client Liaison asserting the customer's readiness to proceed with the migration. This may be provided in the form of a signed checklist or email confirmation. Upon receipt CTS' assigned Project Manager will review and either a) confirm readiness or b) return the checklist for further work. After readiness is confirmed by CTS, migration work and related activities will begin.

All system migrations are coordinated through an overall project schedule. A [Migration Calendar](#) has been published reflecting SDC migration activity.

Document Structure

As agencies progress through the Guide, they will see prerequisite tasks that:

- Must be completed internally by the customer agency
- Must be completed by CTS staff
- Must be completed in coordination with CTS

Each task is prefaced with a table entry that contains a column each for identifying the primary party responsible for completing the work activity, a task number and a relative description. The table below provides a brief sample:

Party	Task #	Task Description
Customer	1	Prerequisite task that must be completed by the customer Agency
CTS	2	Prerequisite task that must be completed by CTS

Each table entry will be followed by a more detailed description of the work to be accomplished for that task. Migration tasks have been organized in a general chronological order.

Please Note: All migration tasks have been built to include a wide range of scenarios and not all tasks apply to every migration – these tasks will be clarified for each firewall with the appropriate party during the planning phase.

Agency Implementation Coordinators will interface with the CTS Enterprise Projects Client Liaison to review any questions regarding this Guide.

Document Scope

There are two SDC projects that include migrations that may impact customers. Those projects are:

- **CTS Move Phase 1** - This project will focus on moving selected CTS equipment that best alleviates the heat issue in OB2. This phase will move the following primary areas:
 - Servers
 - Telecommunications
 - Security
 - Mainframes
 - Network
- **Firewall** - This project will replace aged and over-capacity firewalls. It will also deliver enhanced data security services such as enterprise logging and event correlation, and intrusion detection/intrusion prevention.

This Guide addresses **Firewall** and includes the following:

- **Section 1: MPLS Connectors (Simple Security Policy)**

The following sections are currently in development and will be included in future versions of this Guide:

- **Section 2: MPLS Connectors (Complex Security Policy)**
- **Section 3: Others**

Section 1 – MPLS Connectors (Simple Security Policy)

The following tasks apply to MPLS Connectors (Simple Security Policy) migrations:

Migration Tasks

30 TO 60 DAYS BEFORE MIGRATION

CTS Client Liaison	1	Identify Migration Team
CTS Client Liaison	2	Schedule Migration Planning Session(s)

The CTS Client Liaison must work with the CTS project manager and the AIC to identify the resources required to migrate and validate the firewall. This Migration Team will perform the migration and verification activities.

The CTS Client Liaison will facilitate meetings needed to plan and coordinate the migration.

CTS	3	Conduct Firewall and Data Flow Mapping
-----	---	---

The CTS Enterprise Security Services (ESS) team will work with CTS Network staff to map each customer firewall and data flow. The purpose is to determine if the firewall is still viable and needed.

Both	4	Redesign Environment (if needed)
------	---	---

Some firewalls have dramatic changes and will require additional time and effort for design. If needed the Customer and CTS will need to meet and review to validate the design.

CTS	5	Validate Customer IP Subnets
-----	---	-------------------------------------

The CTS ESS team will work with CTS Network staff to review customer IP subnets to ensure that customer VRF's are not using IPs already in use. This step is taken to avoid potential duplication and subsequent network issues.

Both	6	Create Migration Plan and Back-out Plan
------	---	--

A Migration Plan is needed to guide the migration effort. The Back-out Plan will be used in the event a problem arises that cannot be resolved during the migration window. Escalation contacts and decision making timeframes will be identified as part of the Back-out Plan. The Customer and CTS will meet (e.g. conference call or in person) to review and validate both Plans.

Both	7	Create Test Plan
------	---	------------------

Both CTS and the Customer will develop a Test Plan that will be executed immediately following the migration. The purpose of this is to ensure that customer traffic is flowing and operating as expected after the migration. The Test Plan will include:

- CTS will test to ensure that the firewall services are operating as expected. Testing will include network connectivity via ping, telnet and web browsing.
- Customer will test email (internet check), web browsing (e.g. Google and [Access.wa.gov](https://www.access.wa.gov)). Note: the email client may need to be restarted after the migration and prior to testing email.

Both	8	Schedule Migration
------	---	--------------------

The date and time (window) for the migration must be coordinated with all impacted parties (CTS and the Customer). This becomes the target date of the move.

Several factors should be considered by the customer when determining if the migration schedule meets the customer's requirements. These factors include but may not be limited to:

- user impact,
- migration during or after core business hours,
- staffing,
- maintenance schedules, and
- other changes (e.g. network, system, etc.) occurring at the agency.

As a result, the customer may decide to migrate during the day, overnight, or potentially over the weekend.

1 TO 7 DAYS BEFORE MIGRATION		
-------------------------------------	--	--

CTS Client Liaison	9	Confirm Migration Schedule and Plan (Go/No Go)
--------------------	---	--

The CTS Client Liaison will check-in with the AIC to confirm the schedule and Migration Plan. If needed, any final adjustments will be made and communicated to the Migration Team. The CTS Client Liaison will provide the conference bridge information to the AIC at this time.

MIGRATION DAY

CTS ESS Technical Lead	10	Assemble Migration Team
------------------------	----	--------------------------------

The CTS ESS Technical Lead will assemble the Migration Team to start the process. This is the final go/no go point.

CTS ESS Technical Lead	11	Send Notification of the Start of the Firewall Migration
CTS ESS Technical Lead	12	Initiate the Customer Conference Bridge

The CTS ESS Technical Lead will notify CTS staff and management the start of the firewall migration.

CTS will establish a conference bridge for each migration and encourages customers to participate. The CTS ESS technical lead will initiate the bridge at the scheduled time.

CTS	13	Migrate the Network and Firewall
-----	----	---

The CTS team will start the migration process following the steps identified in the Migration Plan.

CTS TSD Technical Lead	14	Execute CTS Test Plan
------------------------	----	------------------------------

Once the firewall has been migrated to the SDC, the CTS TSD Technical Lead will execute the Test Plan to ensure that the firewall services are operating as expected. If problems occur, CTS resources will participate in troubleshooting and problem resolution.

CTS ESS Technical Lead	15	Notify Customers to Begin Validation or Initiate Back-out
------------------------	----	--

Once CTS staff has verified the firewall is operating as expected, the CTS ESS Technical Lead will notify the customer to begin validation. If issues occur that cannot be resolved within the negotiated migration window, the Technical Lead will notify the customer that the Back-out Plan will be executed and the migration rescheduled.

If the customer has elected to not participate in the conference bridge during the migration, the CTS ESS Technical Lead will notify the CTS Client Liaison with the results. The CTS Client Liaison will then contact the AIC.

Customer	16	Execute Customer Test Plan
----------	----	-----------------------------------

The Customer will conduct their part of the Test Plan and validation. This is needed to avoid unplanned system outages and includes running the test scenarios previously created. If problems occur, the customer will immediately notify the CTS contact to initiate troubleshooting to correct the problem.

Note: the customer is highly encouraged to be available to conduct their Test Plan immediately following their migration to avoid the risk of impact the next business day.

Customer	17	Notify CTS that Test Plan was Successful
----------	----	---

Once the Customer has completed their Test Plan and validation, they will notify CTS of the results of their testing. If successful, the Customer will notify the CTS Client Liaison via email regarding the successful testing. If unsuccessful, the Customer will notify the CTS contact to execute the Back-out Plan.

CTS ESS Technical Lead	18	Send Notification of the End of the Migration
------------------------	----	--

The CTS ESS Technical Lead will notify CTS staff and management the end of the migration.

Appendix A – MPLS Connectors (Simple Security Policy) Migration Checklist

MIGRATION TASKS FOR MPLS CONNECTORS (SIMPLE SECURITY POLICY) FIREWALLS			
30 TO 60 DAYS BEFORE MIGRATION			
Party	Task #	Task Description	Complete?
CTS Client Liaison	1	Identify Migration Team	<input type="checkbox"/>
CTS Client Liaison	2	Schedule Migration Planning Session(s)	<input type="checkbox"/>
CTS ESS	3	Conduct Firewall and Data Flow Mapping	<input type="checkbox"/>
Both	4	Redesign Environment (if needed)	<input type="checkbox"/>
CTS ESS	5	Validate Customer IP Subnets	<input type="checkbox"/>
Both	6	Create Migration Plan and Back-out Plan	<input type="checkbox"/>
Both	7	Create Test Plan	<input type="checkbox"/>
Both	8	Schedule Migration	<input type="checkbox"/>
1 TO 7 DAYS BEFORE MIGRATION			
CTS Client Liaison	9	Confirm Migration Schedule and Plan (Go/No Go)	<input type="checkbox"/>
MIGRATION DAY			
CTS ESS Technical Lead	10	Assemble Migration Team	<input type="checkbox"/>
CTS ESS Technical Lead	11	Send Notification of the Start of the Firewall Migration	<input type="checkbox"/>
CTS ESS Technical Lead	12	Initiate the Customer Conference Bridge	<input type="checkbox"/>
CTS	13	Migrate the Network and Firewall	<input type="checkbox"/>
CTS TSD Technical Lead	14	Execute CTS Test Plan	<input type="checkbox"/>
CTS ESS Technical Lead	15	Notify Customers to Begin Validation or Initiate Back-out	<input type="checkbox"/>
Customer	16	Execute Customer Test Plan	<input type="checkbox"/>
Customer	17	Notify CTS that Test Plan was Successful	<input type="checkbox"/>
CTS ESS Technical Lead	18	Send Notification of the End of the Migration	<input type="checkbox"/>
AGENCY VALIDATION			
Agency:			
Name:			
Signature:			
Date:			